Last modified 03/12/2003. This seems to be a letter I wrote to two undergraduates who were doing projects with me, and who knew Galois theory for finite extensions but needed it for infinite ones.

Dear Chantal and Simon,

Here's a little on infinite Galois theory.

1 Reminder of the finite case

Let F be a fixed ground field and let's assume for simplicity that either F has characteristic zero or F is finite. This simplifying assumption enables us to make the following definition of a "finite Galois extension" below. I follow standard notation: for example E/F means a field E equipped with an inclusion of fields $F \to E$, and I refer to it as "a field extension" or just "an extension".

Definition. *An extension E/F is* a finite Galois extension *if there is a monic polynomial $p(X) \in F[X]$ of degree $n \geq 1$ such that $p(X)$ factors into linear factors $(X-a_1)(X-a_2)\dots(X-a_n)$ in E, and furthermore that E is generated by a_1, a_2,..., a_n (that is, any subfield of E containing F and all of the a_i must be E again).*

Remark. In the bad case where F is infinite but has finite characteristic, one should also ask that $p(X)$ is *separable*, and then this definition is again OK. But let's not go into that.

It's easy to check that E is finite-dimensional as an F-vector space, indeed one can check that the dimension of E over F is at most $n!$, and in practice equality is attained quite often. Let $G = \mathrm{Gal}(E/F)$ denote the set of field automorphisms $\phi : E \to E$ such that $\phi(f) = f$ for all $f \in F$.

We recall two key constructions: if H is a subgroup of G then set

$$E^H = \{e \in E \mid \phi(e) = e \text{ for all } \phi \in H\},$$

a subfield of E containing F, and conversely if K is any subfield of E containing F then set

$$G^K = \{\phi \in G \mid \phi(k) = k \text{ for all } k \in K\}.$$

Now we recall a theorem:

Theorem 1.1 (Fundamental theorem of Galois theory)**.** *(i) G is finite and the order of G is* $\dim_F E$.

(ii) If X is the set of all subgroups of G and Y is the set of all subfields of E containing F then X and Y are canonically in bijection with each other, the canonical map $X \to Y$ being $H \mapsto E^H$ and the canonical map $Y \to X$ being $K \mapsto G^K$. These maps are inverses of one another, that is, if you do first one and then the other, you get back to the element you started with. In particular, Y is finite (because X obviously is) (note that it's not at all obvious that Y is

finite: for example a vector space argument doesn't do it because a 3-dimensional vector space has infinitely many 2-dimensional subspaces).

(iii) (more about the bijection) If H is a subgroup of G and $K = E^H$, then then E is clearly Galois over K (because the same polynomial will work). But I can tell you more: the Galois group $\mathrm{Gal}(E/K)$ *is canonically isomorphic to H, the map being the obvious one (every element of H gives an automorphism of E fixing K and hence an element of* $\mathrm{Gal}(E/K)$*. In particular $[E : K]$ is equal to the size of H by (i) applied to E/K, and hence $[K : F] = [G : H]$.*

(iv) (the normal case) Say H is a subgroup of G and $K = E^H$ is the corresponding subfield of E. Then H is a normal subgroup of G if and only if K is a Galois extension of F (if and only if K is a normal extension of F) and in this case, (unsurprisingly by the last statement of (iii)), $\mathrm{Gal}(K/F)$ *is canonically isomorphic to G/H, the isomorphism being the obvious one: if $gH \in G/H$ then lift to $g \in G$; it turns out that $g : E \to E$ has the property that g sends K to K, and the resulting map $K \to K$ is independent of which representative of gH we choose.*

2 Projective limits.

We just do a special case. Let G_1, G_2, G_3,... be (countably) infinitely many groups, and for each $i \geq 1$ let's say we have a map $\phi_i : G_{i+1} \to G_i$ (in general we could just take a bunch of groups and a bunch of maps between then satisfying various axioms, but let's not get too complicated). The notation for this is "system" is

$$\ldots \to G_3 \to G_2 \to G_1,$$

or just (G_i).

The *projective limit* of this system is a group G, which is written $G = \mathrm{proj}\lim_n G_i$, or $G = \lim_{\leftarrow n} G_i$, and also a collection of maps $\psi_i : G \to G_i$ for all i (although the maps are frequently dropped from the notation), satisfying the following two axioms:

(i) $\phi_i \psi_{i+1} = \psi_i$ for all $i \geq 1$ (the maps ψ_i are "compatible with the system), and

(ii) if H is any group and $\rho_i : H \to G_i$ are any maps which are compatible with the system, then this compatibility is "explained by G" in the sense that there is a *unique* map $\rho : H \to G$ such that $\rho_i = \psi_i \rho$ for all $i \geq 1$.

This is a funny definition, in the sense that I have "defined" a projective limit only by listing some of the properties that it has, rather than building it. The only reason for this is that the actual definition of the projective limit is quite messy, and in fact 9 times out of 10 one only needs properties (i) and (ii) of the definition, rather than the construction. The first time I saw this happening in mathematics was the tensor product, which is "universal for bilinear maps".

To prove that this is a good definition, I now have to do two things: given a system (G_i) I must (1) prove that there is at most one such G, and (2) prove that there is at least one. The proof that there is at most one is just formal: if G and H both worked, then both G and H are compatible with the system,

and (ii) gives maps $G \to H$ and $H \to G$; furthermore (ii) applied with G and G shows that the unique map $G \to G$ compatible with the system is the identity, so the composite $G \to H \to G$ is the identity, as is $H \to G \to H$ so G and H are uniquely isomorphic.

The proof that there is at least one involves building G, and it's not pretty. Firstly look at the product of all the G_i. This isn't it, it's too big. Then look at the subgroup of the product consisting of elements $(g_1, g_2, g_3, \ldots)$ such that $\phi_i(g_{i+1}) = g_i$ for all $i \geq 1$. This turns out to work.

Definition. *A* profinite group *is a projective limit of finite groups.*

Example: $\mathbf{Z}_p = \mathrm{proj\,lim}_n(\mathbf{Z}/p^n\mathbf{Z})$, the p-adic numbers (in fact they are of course a profinite ring!).

Profinite groups have a natural topology, coming from the construction: give the finite groups the discrete topology, the product the product topology (this is no longer discrete!) and the subgroup (which turns out to be closed) gets the subspace topology. So now we can talk about closed subgroups of a profinite group.

3 Infinite Galois Theory

Let E/F be an infinite extension of fields, but assume that E/F is *algebraic*, that is, that every element $e \in E$ is a root of a non-zero polynomial with coefficients in F. Assume again that F is either finite or of characteristic zero. We say that E/F is *Galois* if E is set-theoretically a union of finite Galois extensions of F.

Example: $F = \mathbf{Q}$ and $E = \mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \ldots)$. Note that E is not the union of every quadratic extension of $\mathbf{Q}$, because for example E contains $\sqrt{2}+\sqrt{3}$ which is contained in no quadratic extension of $\mathbf{Q}$, but E *is* Galois over Q as it's the union of $\mathbf{Q}$, $\mathbf{Q}(\sqrt{2})$, $\mathbf{Q}(\sqrt{2}, \sqrt{3})$, $\mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ and so on, and all these are Galois (for example $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ is the splitting field of $(X^2-2)(X^2-3)$ over $\mathbf{Q}$).

If E/F is an infinite Galois extension, and if we now make the additional assumption that E is a countable union of finite Galois extensions of F, which would have been unnecessary if I had set up projective limits more generally, but which is true in all the cases I know other than very pathological ones, then we can write $E = E_1 \cup E_2 \cup E_3 \cup \ldots$, and by replacing E_i by the field generated by E_1 up to E_i if necessary, we can assume that E_{i+1} contains E_i for all i. Write $G_i = \mathrm{Gal}(E_i/F)$, a finite Galois group, and note that by the fundamental theorem, the subgroup H_{i+1} of $G_{i+1} = \mathrm{Gal}(E_{i+1}/F)$ corresponding to E_i is normal, and the quotient G_{i+1}/H_{i+1} is canonically isomorphic to G_i, giving us a canonical map $\phi_i : G_{i+1} \to G_i$.

Definition. $\mathrm{Gal}(E/F) = \mathrm{proj\,lim}\, G_i$.

So an infinite Galois group is a profinite group and in particular has a topology. Let E/F be an infinite Galois extension, that is, E/F is Galois and $\dim_F E = \infty$. Set $G = \mathrm{Gal}(E/F)$. Note that $g \in G$ gives $g_i \in G_i = \mathrm{Gal}(E_i/F)$

for all i, and hence maps $E_i \to E_i$ for all i, and by the compatibility of G with the system, these maps glue together to give a unique well-defined map $E \to E$. Moreover it is not difficult to check that in fact G is, as a group, the group of field automorphisms $E \to E$ which fix F pointwise, although if one defines it this way then one doesn't see the topology of G, which is crucial for the theorem below.

Theorem 3.1 (Fundamental theorem of Galois theory for infinite extensions)**.** *Let E/F be an infinite Galois extension, and set $G = \mathrm{Gal}(E/F)$.*

(i) G is infinite [although typically G is uncountably infinite, and $\dim_F E$ is only countably infinite, so the strict analogue of the finite dimensional (i) is false]

(ii) If X is the set of all closed subgroups of G and Y is the set of all subfields of E containing F, then X and Y are canonically in bijection, with the maps being the same as before (in particular if K is a subfield of E then I am claiming that $\{g \in G : g(k) = k \text{ for all } k \in K\}$ is a closed subgroup of G) (which is actually quite easy once you understand the topology of G).

(iii) If H is a closed subgroup of G then E is Galois over $K := E^H$ and $\mathrm{Gal}(E/K)$ is canonically isomorphic to H. Note that here H can either be finite or infinite, and this will correspond to the dimension of E as a K-vector space being finite or infinite. Again the map is the obvious thing.

(iv) If H is a closed subgroup of G and $K = E^H$ is the corresponding subfield of E, then H is normal iff K/F is Galois and in this case $\mathrm{Gal}(K/F)$ is canonically the quotient group G/H, the map being the obvious one. In particular, H has finite index in G iff K/F is a finite Galois extension.

The proof of this theorem is in two parts: (1) prove the finite case (main theorem of the Galois theory course, goes on for ages), and then (2) just do a little bit of unravelling and deduce the infinite case easily. The point is somehow that if K is a subfield of E then $K_i := K \cap E_i$ is a subfield of E_i, and K is the union of the K_i, and E_i/F is finite so we know all about this from the finite case, and K is determined by all the K_i. All the hard work is in the finite case.

Note that if $G = \mathrm{proj\,lim}_i\, G_i$ then G is a compact topological space, as it is a closed subspace of a product of compact topological space (products of compacts are compact and closed subspaces of compacts are compact). In particular if H is an *open* subgroup of G then writing $G = \coprod_{g \in S} gH$ (and assuming $1 \in S$) we see that all the gH are open, as they are translates of H (this is part of the axioms for a topological group, that translates of opens are open), and hence $G - H$ is a union of open sets $\coprod_{1 \neq g \in S} gH$ so it's open, so H is closed, and we have also covered G by disjoint open sets so by compactness we must have S finite, so H has finite index. One now can check that the bijection between closed subgroups of G and subfields of E continaing F induces a bijection between open subgroups of G and subfields of E containing F and which are finite-dimensional over F.

Example: if $F = \mathbf{Q}$ and $E = \mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \ldots)$ then $\mathrm{Gal}(E/F)$ is a countably infinite direct product of copies of $\mathbf{Z}/2\mathbf{Z}$ (the proof is a long exercise and you might need to know things like $\sqrt{p}$ is not in the field generated by $\sqrt{n}$ for all $n < p$, this follows because $\mathbf{Q}(\sqrt{p})$ is ramified at p but $\mathbf{Q}(\sqrt{n})$ isn't).

Example: if $F = \mathbf{Q}$ and E is the algebraic numbers in $\mathbf{C}$ then E is frequently written as $\overline{\mathbf{Q}}$, and E/F is an infinite Galois extension, and the Galois group is frequently called $G_{\mathbf{Q}}$. It's very big and understanding the representations of this group is at the heart of number theory. Note that every prime ramifies in $\overline{\mathbf{Q}}$, infinitely badly! $\overline{\mathbf{Q}}$ is the union of every number field.

Example: One gets much more reasonable examples if one only considers number fields with certain reasonable properties. For example if S is a finite set of primes then a much more reasonable extension of $F = \mathbf{Q}$ is the subfield E of $\overline{\mathbf{Q}}$ which is the union of all the number fields which are unramifed at p for all p not in S. People write $E = \mathbf{Q}_S$ sometimes. If S is empty then $E = F = \mathbf{Q}$ but if S contains a prime p then already E is infinite because it contains $\mathbf{Q}(\zeta_{p^n})$ for all $n \geq 1$ (it turns out that $\mathbf{Q}(\zeta_m)$ is ramified only at primes dividing m). The group $\mathrm{Gal}(\mathbf{Q}_S/\mathbf{Q})$ has some nice conjuacy classes: if q is a prime not in S then all the number fields used to build $\mathbf{Q}_S$ are unramified at q so all the Galois ones have Galois groups containing conjugacy classes called Frob_q, and because the definitions are all so natural, one checks that they glue together to give a conjugacy class Frob_q in $\mathrm{Gal}(\mathbf{Q}_S/\mathbf{Q})$.

Example: if F is a field and E_n is a Galois extension of F with Galois group $\mathbf{Z}/p^n\mathbf{Z}$, and if all the E_n are contained in some big field, and E is the union of the E_n, then $\mathrm{Gal}(E/F)$ will be $\mathbf{Z}_p$, the projective limit of $\mathbf{Z}/p^n\mathbf{Z}$. For example F could be $\mathbf{Q}(\zeta_p)$ for some $p > 2$ and E_n could be $\mathbf{Q}(\zeta_{p^{n+1}})$.

Example: if E/F is an infinite Galois extension and $G = \mathrm{Gal}(E/F)$ and $\phi : G \to H$ is a continuous map from G to a group with the discrete topology (for example $\mathrm{GL}_2(\overline{F}_p)$ or $\mathrm{GL}_2(\mathbf{F}_p)$) then $\{1\}$ is an open subgroup of H so $\ker(\phi)$ is an open subgroup of G so ϕ factors through $G/\ker(\phi)$ which is $\mathrm{Gal}(K/F)$ for K some *finite* Galois extension of F.

I am a bit lazy and haven't proofread this document much, so hope it's OK.

Kevin